PQC enhancement for EAP-AKA’

draft-ar-emu-pqc-eapaka-00

IETF 119 Brisbane, 19th March, 2024

Aritra Banerjee (Nokia)

K Tirumaleswar Reddy (Nokia)

Motivation

- EAP-AKA' FS [I-D.ietf-emu-aka-pfs] provides updates to [RFC9048] with an optional extension that offers ephemeral key exchange using the traditional ECDHE key agreement algorithm for achieving perfect forward secrecy (PFS).

- However, it is susceptible to future threats from CRQCs, which could potentially compromise a traditional ephemeral public key.

- If the adversary using CRQC has also obtained knowledge of the long-term key and ephemeral public key, it could compromise session keys generated as part of the authentication run in EAP-AKA'.

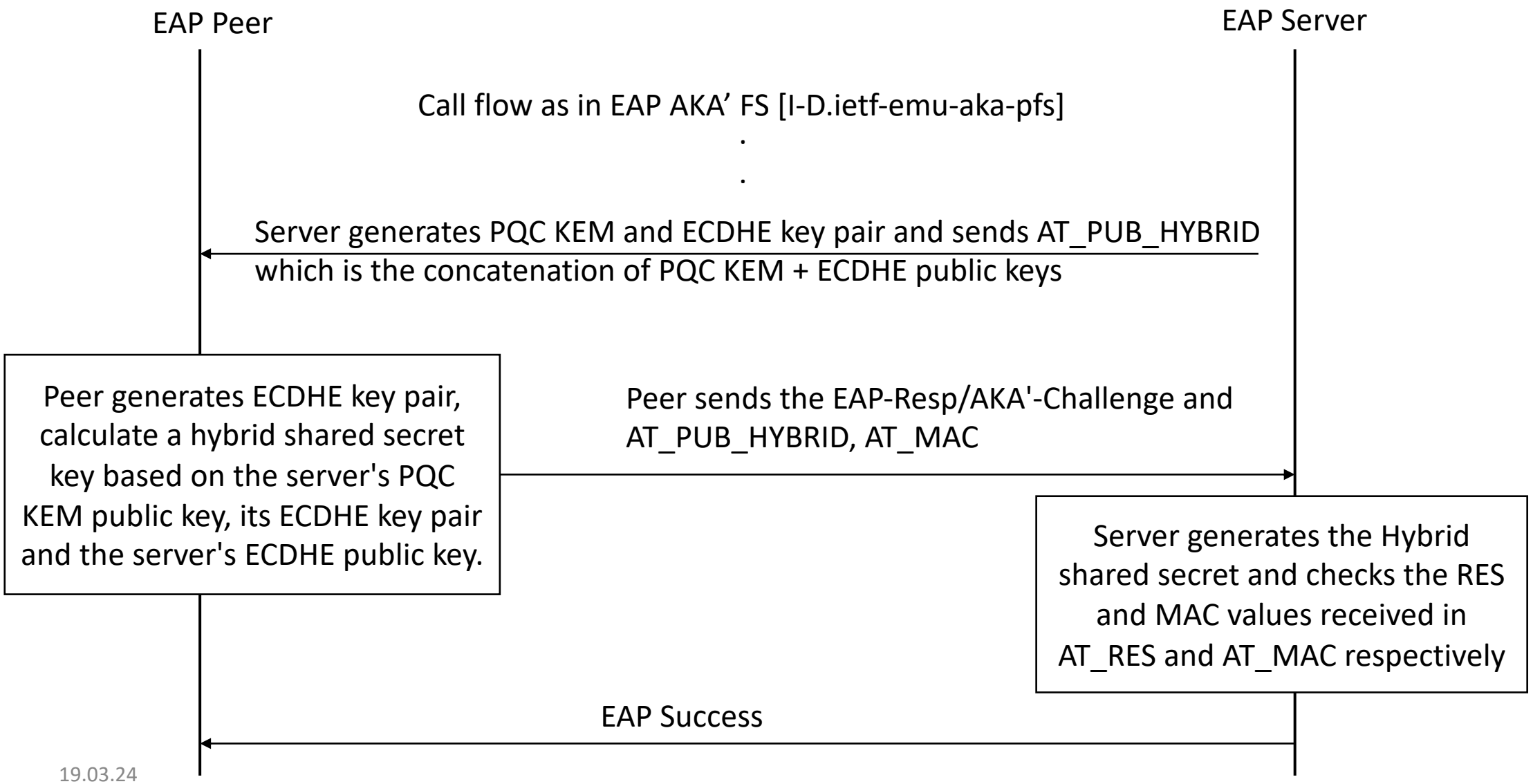
HPKE

- The HPKE specification provides a variant of public key encryption of arbitrary-sized plaintexts for a recipient public key.

- HPKE (Hybrid Public Key Encryption) emerged in the IETF as a prominent public key encryption scheme
  - https://www.rfc-editor.org/rfc/rfc9180.html (Developed by CFRG in IRTF)
  - Used by several protocols Oblivious HTTP, Encrypted Client Hello in TLS, MLS

- HPKE interfaces are friendly to hybrid encryption

Overview of the protocol



Generating Hybrid Master Key

- MK = PRF'(IK'|CK',"EAP-AKA'"|Identity)
- HYBRID_SHARED_SECRET, enc = Encap(pKR) MK_HYBRID = PRF'(IK'|CK'| HYBRID_SHARED_SECRET,"EAP-AKA' FS"| Identity)
- K_encr = MK[0..127]
- K_aut = MK[128..383]
- K_re = MK_HYBRID [0..255]
- MSK = MK_HYBRID [256..767]
- EMSK = MK_HYBRID [768..1279]

Hybrid Key Generation

- The HPKE protocol for general purpose post-quantum KEM in [draft-connolly-cfrg-xwing-kem-01] is used
- sk1, pk1 = GenerateKeyPair(X25519)
- sk2, pk2 = GenerateKeyPair(ML-KEM768)

PQC KEM Public key (pk2), private key (sk2) pair and the ECDH public key (pk1), private key (sk1) pair is generated by the server

Hybrid Encapsulation

- Encapsulate (concat(pk1,pk2)) = (enc, ss)

"enc" is the concatenation of the encapsulated key from ECDH and ciphertext from PQC KEM whereas "ss" is hybrid shared secret key.

Hybrid Decapsulation

- Decapsulate(enc, concat(sk1,sk2)) = ss

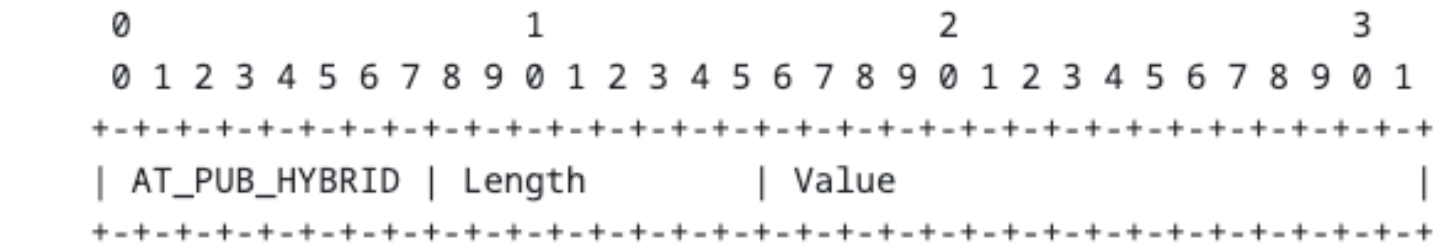
The generated ss from Decapsulate is the hybrid shared secret key derived from PQC KEM and traditional ECDH.

Overview

- A new attribute, AT_PUB_HYBRID, is defined to carry the public key, which is the concatenation of traditional and PQC KEM public keys from the EAP server.
- The AT_PUB_HYBRID attribute will carry the encapsulated key, which is formed by concatenating the encapsulated key (enc) from the traditional KEM algorithm and the ciphertext (ct) from the PQC KEM Encapsulation function from the EAP peer.
- The AT_KDF_FS attribute is updated to indicate the HPKE KEM and HKDF for generating the Hybrid Master Key MK_HYBRID.
- The Hybrid key derivation function will be included first in the EAP-Request to indicate a higher priority than the traditional key derivation function.

AT_PUB_HYBRID attribute

The format of the AT_PUB_HYBRID attribute is shown below.



Value:

EAP-Request: It contains the public key, which is the concatenation of traditional and PQC KEM public keys from the EAP server.

EAP-Response: It contains the encapsulated key, which is formed by concatenating the encapsulated key (enc) from the traditional KEM algorithm and the ciphertext (ct) from the PQC KEM Encapsulation function from the EAP peer.

Next Steps

- Comments and Suggestions are welcome